Homeland Security Affairs

Volume I, Issue 2 2005 *Article 2*

2005

Homeland Security Capabilities-Based Planning: Lessons from the Defense Community

Sharon L. Caudle*

*US Government Accountability Office, caudles@gao.gov

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Homeland Security Capabilities-Based Planning: Lessons from the Defense Community	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

Homeland Security Capabilities-Based Planning: Lessons from the Defense Community*

Sharon L. Caudle

Abstract

Beginning in 2004, the Department of Homeland Security (DHS) began to define and implement a national domestic all-hazards preparedness goal, intended to improve the nation's preparedness for national catastrophes, including terrorist attacks. DHS's approach was capabilities-based planning (CBP), adopted from the Department of Defense (DoD). This article illustrates several components important for CBP implementation to contrast with DHS's approach. These components range from setting out the business case for CBP adoption to necessary organizational and cultural enablers. The article concludes with CBP implementation challenges because of differences between homeland security and the defense community.

AUTHOR BIOGRAPHY: Dr. Sharon Caudle is an assistant director with the U.S. Government Accountability Office's (GAO) Homeland Security and Justice Team. She specializes in homeland security and national preparedness strategic policies, programs, standards, and management. She currently serves on the American National Standards Institute's Homeland Security Standards Panel steering committee and the technical committee for the national standard for disaster management, emergency management, and business continuity. She is also a senior fellow with the George Washington University's Homeland Security Policy Institute and is an adjunct faculty for the Office of Personnel Management's Development Centers and The George Washington University. She earned her Master degree and doctorate in public management from The George Washington University in Washington, DC, and recently earned a Master degree in homeland security and homeland defense from the School of International Studies, Naval Postgraduate School, in Monterey, CA.

KEYWORDS: capabilities-based planning, performance management

---

*This article represents the views of the author and not those of the Government Accountability Office.

INTRODUCTION

In 2003, President Bush's Homeland Security Presidential Directive 8 (HSPD-8) required the Department of Homeland Security (DHS) Secretary to develop a national domestic all-hazards preparedness goal. The intent was to establish measurable readiness priorities and balance threats and consequences with resources required to prevent, respond to, and recover from them. The goal would include readiness measures, standards for preparedness assessments and strategies, and a system to assess the nation's overall preparedness to respond to major events, especially terrorist acts.

Paying attention to the goal and related readiness priorities, particularly at the state and local levels, is vital, for at least one simple reason—federal funding. Under the directive, state all-hazard preparedness strategies consistent with the national preparedness goal will determine federal preparedness assistance.[1] This direction was affirmed when Congress subsequently cited HSPD-8 for preparedness requirements and funding in the fiscal year 2005 DHS appropriations' language. The National Intelligence Reform Act of 2004 also required DHS to set national performance standards and ensure state homeland security plans' conformance with those standards.

Responding to the HSPD-8 mandates, DHS adopted a capabilities-based planning approach (CBP) from the United States Department of Defense (DoD). This article describes the approach, implementation practices from the DoD experience, and contrasts with the DHS strategies.

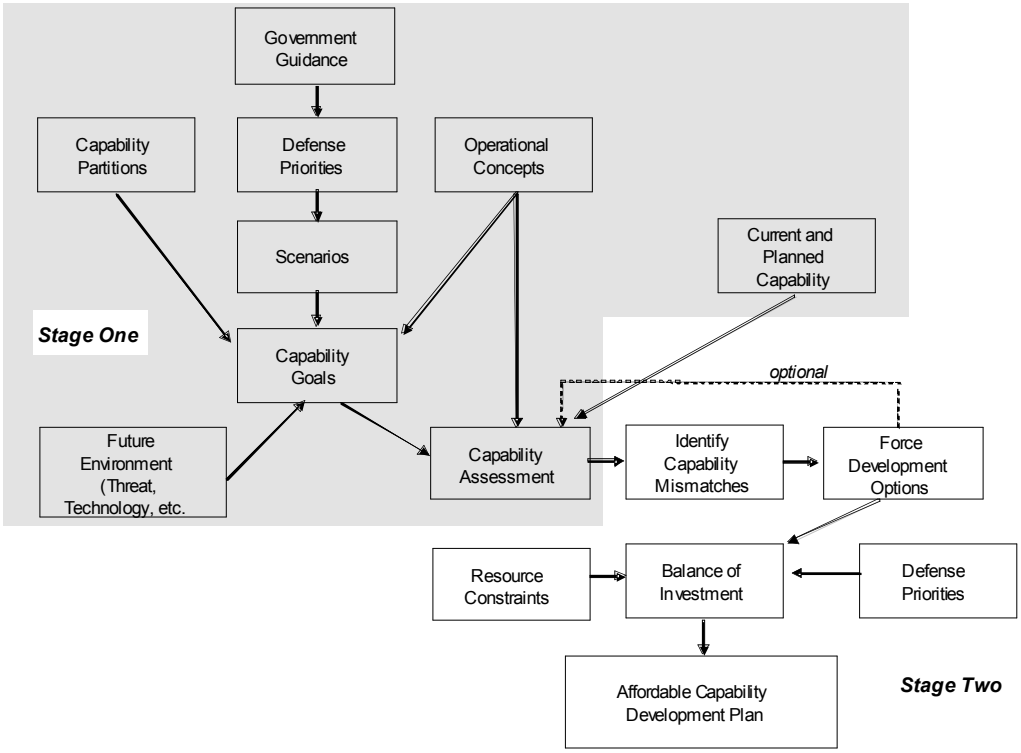
CBP MODEL FOR HSPD 8 IMPLEMENTATION

Capabilities-based planning is one approach that is intended to manage risk, set specific preparedness goals and priorities, make investment choices, and evaluate preparedness results. Proponents describe CPB as developing the means—capabilities—to respond to a wide range of potential challenges and circumstances while mindful of costs and sustainability. CBP uses intelligence, strategic studies, and experiences to describe potential future threats and specific event or longer-term scenarios. The scenarios are used to define specific capabilities through an analytical framework starting with mission objectives and measures of strategic and operational success and ending with an assessment of options on factors such as risk. Choices consider capability tradeoffs and impacts at multiple levels within and across organizational components.[2]

All member nations of the defense community's Technical Cooperation Program (TCP)—Australia, Canada, New Zealand, United Kingdom, and United States—use capability concepts for long-term future defense force structure planning. The central audience for the defense community's CBP is the "combatant commander" who must achieve specific missions. The TCP's generic CBP process chart, shown in Figure 1,

starts with overarching guidance, identifies capability gaps, explores options, and ends with an affordable investment plan.[3]

Figure 1. Generic CBP Process Chart



DEFENSE CBP COMPONENTS AND DHS IMPLEMENTATION

My review of the defense community's CBP experience represented by the TCP highlights several components important for CBP implementation to contrast with DHS's approach and provide "lessons learned" useful for future CBP implementation.[4] In the following sections, I describe these components and briefly contrast them with DHS's efforts to date. Table 1 highlights the defense components and DHS efforts.

Table 1. DHS Approach and the Defense Components

Components	DHS Progress
Business Case for CBP Adoption: *Justify organizational commitment and investment*	Business case stated in terms of national preparedness in HSPD-8 and now in legislation; clear business case still to be made for adopting CBP.
Strategic, Cascading Policy Goals: *Use top-level government guidance that cascades goals into strategic policy and operational documents and into CBP.*	Multiple sources of policy goals including national strategies, HSPD-8 and other presidential directives, the National Response Plan, and the National Incident Management System; integrated, single-source policy document for homeland security and national preparedness not yet available.
Stakeholder Ownership: *Ensure stakeholder involvement, collaboration, and perspective-sharing.*	Inconsistent attention paid to state and local entities as primary stakeholders; primarily federal approach used in consultation with, not collaboration with those entities. Private sector stakeholders yet to be closely involved.
Top Leader Ownership: *Ensure top leader support, involvement, and decision-making.*	Federal leadership within DHS appears supportive; top leadership from other stakeholders still evolving. Decision-making processes not transparent and apparently fragmented.
Specific Management Decision-Making Process: *Design and implement CBP decision process that captures mission tasks and capabilities, their priority, how they relate, solutions, and resource allocation.*	Process has evolved over time but is not formally structured with clear responsibilities, decision-making roles, and integration into stakeholders strategic planning, budgeting, program evaluation, and corrective action. Interim documents extend the process.
Risk Assessment Approach: *Use risk assessment in the CBP management process to determine investments.*	Risk assessment is not well-defined and presented as an integral part of DHS CBP decision-making similar to the defense communities.
Different Planning Horizons: *Incorporate different planning horizons into CBP to stage the development of capabilities.*	No expression of planning horizons to date; DHS has promised to evolve CBP and planning horizons may be part of the evolvement.
Mission-Based, Phased Scenarios: *Have the right scenarios on which to base planning and/or exercises*	Selection of 15 scenarios for planning; concern the scenarios are much too focused on terrorism in contrast to a clearer all-hazards approach and do not include different timeframes, including very long term.
Capability Development and Standard Categories: *Provide guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate.*	Limited guidance on how to develop capabilities; capability categories still in process; no clear direction provided as to what is the best way to structure the capabilities for use by most entities.
Decision Rules for Lists: *Establish clear rules for the development of task lists and capability lists.*	Rules for development not explicit; changing categories and elements.
CBP Evolution: *Evolve CBP depending on planning applications and developing maturity.*	Policy timeframes have precluded a more evolutionary approach to CBP and addressing differing maturity in capability areas.
CBP Enablers: *Consider organizational and cultural enablers to support CBP adoption.*	Enablers may be recognized but have not been adequately addressed; process characterized by rapid spiral development with extremely limited timeframes for consideration.

Business Case for CBP Adoption

First, CBP adoption requires a strong business case to justify the organizational commitment and investment. In the defense communities, the business case grew primarily out of the need to shift defense planning from a "threat-based" model to a "capabilities-based" model. Instead of planning for large conventional wars in a few distant theaters under the threat-based model, the 2001 Quadrennial Defense Review proposed identifying capabilities that relied on surprise, deception, and asymmetric warfare to deter and defeat adversaries.

DoD used threat-based planning since DoD instituted the Planning, Programming, and Budgeting System in 1962. However, threat-based planning meant strong response to a few situations while largely ignoring all other potential challenges. DoD's threat-based approach and illustrative official planning scenarios for major theater wars served as specifications, defining necessary and sufficient characteristics of the force structure, thereby leading to consistent support of current programs. The approach only considered conventional-wisdom threats and point-in-time versions of detailed scenarios, as though the circumstances of future conflict could be predicted. In the foreword to the Joint Operations Concepts, Secretary Rumsfeld said a capabilities-based approach would focus more on how the United States would defeat an adversary's broad array of capabilities instead of identifying who the adversaries were and where they might threaten joint forces or United States' interest.

While addressing the limitations of threat-based planning was the primary business case for DoD's adoption of CBP, there were other reasons too. CBP attempts to break down traditional single-service stovepipes allowing systems and concepts from multiple services to achieve capabilities. A joint focus encourages decisions with broad defense force goals in mind instead of considering their own service. CBP also compares options for achieving the same capability in an integrated fashion. Before CBP, acquisition requirements often were developed, validated, and approved as stand-alone solutions to counter specific threats or scenarios with systems integration forced at the end. The result was duplication, poor spiral acquisition practices, and problems in prioritizing joint warfighting needs. CBP links procurement decisions to strategic goals and provides an audit trail for accountability.

Thus, the defense community experience suggests the adoption of CBP requires a strong business case to justify the organizational commitment and investment, such as flexibility in addressing current and future adversaries and their strategies. For homeland security, DHS officials assumed there would be overwhelming state and local support of a national preparedness goal simply because it was mandated in HSPD-8. Beyond this almost "motherhood and apple pie" argument, very little attention was paid to significant benefits that might result, such as clearly defined levels of preparedness understandable across many organizations and useful for funding decisions. In addition, a clear business case was not made in support of an all-hazards approach under the national goal. The goal's implementation clearly stressed counter-terrorism, with all-hazards a secondary emphasis.

Strategic, Cascading Policy Goals

A second component is establishing specific strategic policy goals from top-level government guidance to derive high-level capability objectives. These policy goals support the use of top-level doctrine or some overarching operational concepts that consider the way a force will fight. Moreover, these goals cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs. For example, the foundation for Canada's CBP was an early White Paper that defined governmental expectations, leading to a Strategy 2020 document that articulated the national defense vision. In turn, the Canadian Forces concept of force employment was crafted to describe how the national defense vision would be delivered. Force planning scenarios illustrated where and when the concept of employment would be applied, finally leading to Canada's capability goals matrix and Canada Joint Task List (CJTL) for CBP. In the United Kingdom, a defense white paper also set out the need to defend against future principal security challenges such as international terrorism, weapons of mass destruction (WMD) proliferation, and weak and failing states. The Australia Department of Defence also relied on a white paper on the future of Australia's defense force.

A similar process occurred in DoD in planning for joint processes and in individual services. DoD built its strategic framework to defend the nation and secure a viable peace around four defense policy goals—assuring allies and friends, dissuading future military competition, deterring threats and coercion against U.S. interests, and if deterrence failed, decisively defeating any adversary. These strategic policy goals are further defined in other documents. For example, within DoD joint force decision-making concepts – Joint Operations Concepts, Joint Operating Concepts, Joint Functional Concepts, and Joint Integrating Concepts – are translated into a capability level of detail, often using a time frame of 10 to 20 years into the future. Military judgment is applied to those concepts to validate what collection of attributes and measures are needed, and thus a standard for critical functional areas. Current programs are mapped against that standard to compare current capabilities against the standard, propose alternatives, choose a specific capability, and then move that decision into the investment strategy.

In summary, specific policy goals, derived from top-level government guidance, should cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs. The National Strategy for Homeland Security provided the most central statement of homeland security intent, but was written largely in support of the formation of DHS. It was joined by other sources of national policy goals, including other national homeland security-related strategies, HSPD-8 and other presidential directives, federal agency strategic plans, regulations and policy guidance, the National Response Plan, and the National Incident Management System. In large part, these various documents are statements of federal perspectives because no clear mechanism exists to produce top-level "national" guidance that is accepted and applicable across all levels of government, non-governmental organizations, and the private sector. Unlike what appears to be the case in the defense communities, these various federally-developed national policy documents stand alone. They have not been systematically integrated into a cohesive policy whole. That may be the role envisioned for the national preparedness goal and related guidance, but its current construction will not meet that need. In some cases, there are conflicting objectives and requirements

across the policy documents. DHS could solve this problem with a single-source policy document for homeland security and national preparedness.

Stakeholder Ownership

A third component is ensuring stakeholder ownership, especially important for joint planning and operations. The TCP says that one of the first requirements for successful implementation of CBP is stakeholder involvement, described in collaborative terms. Stakeholders generally control the information, resources, and authority required to support CBP, and their requirements must be considered from the outset. Key stakeholders—those responsible for identifying and deploying the capability envelopes—will eventually control the CBP process, and it is important that they have ownership of it. Each stakeholder should have an understanding of the perspectives of other stakeholders and an appreciation of different, if not competing, requirements. Defense planners should be engaged at all levels. As with other components, the decision-making process can help build in stakeholder ownership. For example, the U.S. Air Force (USAF) uses its decision process to secure "joint acceptance" of capability selections.

To summarize, the defense community experience shows that the stakeholders should own the process and take responsibility for its use and outputs. Stakeholders generally control the information, resources, and authority required to support CBP. For homeland security, DHS attempted to include stakeholders such as state and local government officials, national associations, and other federal agencies involved in homeland security. However, instead of taking a partnering, collaborative approach, DHS used consultants to develop voluminous draft material and then asked for stakeholder reaction. DHS justified consultation rather than partnership on the tight national goal implementation timeframes in HSPD-8 and its requirement for federal development in consultation with others. The end result has been "push back" from key state and local stakeholders, confusion about intent and requirements, and lack of understanding of CBP and what it is intended to do. In hindsight, of course, a better approach would have been to partner and take a less complex approach to implementation if the HSPD-8 implementation timeframes could not be changed.

Top Leader Ownership

Another component is top leader support, involvement, and decision-making—ownership—for the CBP process. DoD's Joint Integrating Concepts (Joint Concepts) are delivered with a detailed scenario, concept of operations (CONOPS), and a list of tasks with measures for a Functional Capabilities Board (Board) to perform a capabilities based assessment on each Joint Concept and perform a data call to services to match Joint Concept tasks to current, programmed, and planned systems. Each Board is a key decision-making body.

Only the high-level Joint Requirements Operation Council can charter a Board. The Boards ensure new capabilities are conceived and developed in a joint warfighting context and proposals are consistent with an integrated joint force. They also organize, analyze, and prioritize capabilities proposals, oversee the development and updating of functional concepts, and ensure integrated architectures reflect the functional areas. Each Board assesses the Joint Concept against the baseline scenario provided by the author, and then may run it against additional Defense planning scenarios to refine the conditions

and standards for each task and aggregate capability. The CBP output is a weighted list of capability needs, gaps, and excesses.

In 2000, the USAF began developing six CONOPs to support its contribution to the joint defense strategy. All USAF operations, programming, and budget decisions in turn are designed to support the capabilities defined by the CONOPs. Six new CONOPS divisions on the USAF Air Staff in the Operations Requirements Directorate were created to connect CBP around these CONOPS. Each of the USAF's six CONOPS has an assigned advocate called a Champion responsible for the capabilities the USAF has, or needs to develop. The CONOPS Champions play a key role in mitigating risk throughout CONOPS development. They are charged with overseeing the entire development process and for communicating issues to senior leadership. CONOPS assessment and analysis is conducted by subject matter experts under the critical jurisdiction of each Champion. CONOPS Champions will integrate priorities among capabilities for review by the USAF corporate structure and participate in the Joint Requirements Oversight Council via USAF challenges. Oversight action and challenges ensure all CONOPS capabilities are addressed at the Boards to help ensure all programs are jointly accepted.

Therefore, the defense community experience demonstrates that top leadership support, involvement, and decision-making are critical to CBP success. For defense, support has truly started at the top of cabinet departments and ministries and been sustained. Top military and civilian officials are responsible for CBP and are held accountable for its operation. In contrast, DHS never established similar top leadership authorities and decision-making processes for CBP. This could be corrected by establishing a formal board, similar to the DoD Functional Capabilities Board for top CBP leadership. Such a board would include federal, state, and local representation with national state and local associations tasked to name representatives.

Specific Management Decision-Making Process

A fifth component is a well-designed and implemented decision process for CBP. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, solutions to meet those needs, and allocation of resources. For example, the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System, and the Planning, Programming, Budgeting, and Execution process form DoD's three principle decision support processes to transform the military forces to support the National Military Strategy and the Defense Strategy. The JCIDS provides an enhanced methodology to identify and describe gaps and redundancies in capabilities, prioritize capability proposals, and improve collaboration with other departments and agencies. The goal is to ensure that the joint force has the capabilities necessary to perform across the range of military operations.

JCIDS analysis begins with a Functional Area Analysis that identifies the operational tasks, conditions, and standards needed to achieve military objectives. As input, it uses the national strategies, Joint Operating Concepts, Joint Functional Concepts, Joint Integrating Concepts, Integrated Architectures, the Universal Joint Task List, and the anticipated range of broad capabilities that adversaries might employ. Output consists of the tasks to be reviewed in the follow-on Functional Needs Analysis that assesses the ability of the current and programmed joint capabilities to accomplish the tasks that the functional area analysis identified, under the full range of operating conditions and in

compliance with designated standards. The needs analysis produces a list of capability gaps or shortcomings that require solutions and indicates the time frame in which those solutions are needed. A Functional Solution Analysis follows, which is an operationally-based assessment of potential approaches to solving (or mitigating) one or more of the capability gaps (needs) identified in the Functional Needs Analysis.

A capabilities review and risk assessment (CRRA) step following a functional needs analysis is the most important step for the Air Force. In the CRRA, capability measures are developed from a variety of analysis tools such as current intelligence estimates, modeling and simulation, and wargaming. Measures of effectiveness are assigned to all levels of required capabilities within a master capabilities list to score how well the USAF performs. Scenarios are selected to assess the USAF's ability to deliver effects needed. Scenarios from the Defense planning scenarios are used and further refined by guidelines in the National Security Strategy and the National Military Strategy. The scenarios also are modified by more demanding requirements known as stressors to craft broad spectrum capabilities. Analysis determines a definition of problems and capability shortfalls, presented to USAF senior leadership for decision-making and resource allocation.

Thus, the defense community experience indicates a well-designed and implemented decision process for CBP is an element for success. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, and solutions for meeting those needs. Homeland security, however, does not yet have a process similar, for example, to DoD's Joint Capabilities Integration and Development System. The homeland security CBP process at this point is not formally structured with clear responsibilities, decision-making roles, defined steps and expected inputs and outputs, and melding into formal organizational planning, budgeting, and procurement decisions. It is not clear how CBP will be seamlessly integrated with existing management approaches for government agencies, non-governmental organizations, and private sector companies. The linkage from results expectations to budgeting is particularly problematic for funders such as boards of directors, city councils, state legislatures, and Congress must accept and act on CBP's analytical framework and its products for decision-making.

Risk Assessment Approach

A sixth component is using risk assessment in the CBP management process. A key tenet of CBP is addressing affordability and sustainability, which means that not all capabilities can be deployed or maintained. Affordability and sustainability requires addressing risk tolerances and priorities for capability development and deployment, and assessing capabilities and their impacts over time. Balancing investments in CBP will require deletions and additions in elements such as force development as part of risk and priority setting.

For example, the DoD developed a broad approach to risk management intended to ensure the defense establishment is sized, shaped, postured, committed, and managed to accomplish defense policy goals. Managing risk means changes in operating practices and military and civilian personnel systems, business practices, and infrastructure. These dimensions reflect DoD's experiences over the last decade in attempting to balance strategy, force structure, and resources. The risk management framework gives DoD the

ability to consider capability tradeoffs among fundamental objectives and fundamental resources constraints.

The framework is made of four related dimensions: force management, operational, future challenges, and institutional. Force management is the ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing operational tasks. Operational is the ability to achieve military objectives in a near-term conflict or other contingency, with risk management considering not just additional force structure, but also assessing changes in capabilities, concepts of operations, and organizational designs to help reduce risk. A future challenge is the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid- to long-term military challenges. The last dimension is institutional, the ability to develop management practices and controls that use resources efficiently and promote the effective operation of the defense establishment.

Periodic assessment of existing and planned capabilities is part of ongoing risk assessment. The TCP notes some nations that are practicing CBP will assess capabilities three or four times over an approximate fifteen year period. For example, the Canada Department of National Defence uses a capability goals matrix to rank capabilities. There are four levels in the Canadian matrix—military strategic, operational, and tactical, with the operational level divided to identify goals in the domestic and international context. The capability areas are rated as to importance (high, medium, and low) to the Department of National Defence and the Canadian Forces to achieve their overarching defense mission. To reach high capability, the Department of National Defence and the Canadian Forces must be capable of exerting effective, unilateral defense ability in the majority of the applicable Canadian Joint Task List sub-tasks associated with that capability area. The capability must be high and unilateral because it cannot be delegated to another nation or because experience and strategic circumstances dictate that high is the minimum acceptable level for overall success and risk management.

Medium level capability goals, less easily defined, are those where an effective capability in most of the applicable sub-tasks is considered important and may also result from a conscious decision to assume some risk in that capability area. For example, the Canadian Forces need to conduct joint and combined operations effectively and possess interoperability with major allies. Canada's risk assessment considers joint and combined operations as separate concepts. "Jointness" is the art of combining capabilities from different military services to create an effect that is greater than the sum of the parts. However, not all military functions or capabilities need to be joint: some will be combined. Canadian units more frequently will be combined (interoperate) with the units of another nation of similar capabilities, producing a larger formation and complementary capabilities coordinated in a specific situation. Units may also need to assume a significant leadership role for medium capability goals, although this will not normally be necessary.

A low capability goal indicates a minimum level of capability, depending on a specific strategic situation or an assessment of benefits in seeking a higher capability level for an assigned defense mission compared to costs. Under a low capability goal, Canadian units must be able to take part in joint or combined operations, but not assume a leadership role.

In sum, the defense community experience points out that risk assessment is part of the CBP management process. Risk assessment addresses affordability and sustainability, and thus risk tolerances and priorities for capability development and deployment and their impacts over time. Assessment of risk is built into scenarios, capabilities review, and a consideration of benefits and costs. Measurement systems are viewed as very important. Other than scenario development and directions for states and localities to consider what is appropriate for their jurisdictions, risk assessment is not well-defined and presented as an integral part of homeland security CBP decision-making. Measures and evaluation systems are still in development. Moreover, it will be difficult to develop and implement regional approaches where core capabilities can be supported and supplemented by other jurisdictions in the region. Political considerations may encourage jurisdictions to have a complete set of core preparedness activities rather than rely on other entities. As a result, many jurisdictions will be engaged in parallel activities within their own risk decisions, and there may be little opportunity to learn from one another or share resources as part of an overarching risk management approach.

Different Planning Horizons

An additional component is incorporating different planning horizons into CBP to stage the development of capabilities. The timeframes should cover a sufficient span for action and changes to take effect, and then allow an assessment of risk over time. To illustrate, the Canada Department of National Defence envisions three planning horizons, each with a different focus for CBP. Horizon One is for a maximum of five years and seeks to deliver capability in already identified ways. Horizon Two is for five to fifteen years and focuses on delivering already identified capabilities in better ways. Horizon Three is for ten to thirty years and determines if capabilities are needed in the anticipated future, in addition to exploring radically new ways of delivering capabilities. The time period is deliberately overlapping for Horizons Two and Three.

Canada describes the first horizon as the most detailed because it executes an already developed plan and shapes near term program aspects. It requires detailed programming of resources, determining if plans are unfolding as required, and developing the appropriate level of capability. The second horizon optimizes how best to do what already is generally understood and ensure that introducing a more effective way of delivering a known capability transitions seamlessly into the more detailed plans from Horizon One. The third horizon is the most challenging as it deals with introducing fundamental changes in the way a capability will be delivered and determining what developments promise to deliver the future necessary capabilities.

Similarly, DoD describes the need for a two-pronged view of implementing CBP—maintaining a military advantage in key areas while developing new areas of military advantage and denying asymmetric advantages to adversaries. Thus, it entails adapting existing military capabilities to new circumstances, while experimenting with the development of new military capabilities. More specifically, force development planning solves future capabilities by asking what top-down investment guidance is needed to address future strategic challenges. Force development decisions also consider what DoD can provide in achievable technologies and methods of the future force. In contrast, force employment decisions involve planning for today's events, such as strategic

decisions as to how best to manage and posture DoD assets to support national interests and mitigate risks.

In sum, the defense community incorporates different planning horizons into CBP to stage the development of capabilities for the near, medium, and long term. The homeland security approach at this stage does not appear to have any similar expression of planning horizons. The fifteen homeland security planning scenarios address an event in the "here and now" (bombings and bioterrorism) with an emphasis on national priorities. DHS has promised to constantly assess and change CBP and thus the needed planning horizons may yet be addressed. However, lack of attention to capabilities for varying horizons may result in implementing capabilities that may be appropriate next year, but not five years from now. The result is poor investment portfolio planning and creating capabilities that may be obsolete or require extensive updating in a short time period. The focus on national priorities may obscure or delay an emphasis on more valued planning horizons that anticipate possible future scenarios.

Mission-Based, Phased Scenarios

The eighth component is having the right scenarios on which to base planning and/or exercises. Defense capability should be assessed using plausible situations encapsulated in planning scenarios. These scenarios provide the context of CBP and should cover the full spectrum of military activities. The scenarios help develop realistic capability goals and the provision of a defense force meeting government requirements at a minimum cost. In addition, as mentioned earlier, scenarios should provide a series of time frames to facilitate capability assessment through time as part of risk assessment, rather than at a single arbitrary point in the future. Scenarios also should be used in combination to assess simultaneous operations.

Scenario types can be on a spectrum, ranging from real world planning scenarios to generic scenarios. Whichever type of scenarios are used, the scenarios should reflect the type of tasks that the government may want its defense force to undertake. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur.

Australia uses one or more strategic scenarios to identify a capability requirement and then operational scenarios determine the operational requirements for a proposed capability. Strategic scenarios represent strategically endorsed scenarios, high-level descriptions of situations with a brief history of preceding events and their context. Each scenario typically will describe a conflict situation, an opposing force, a military setting, a theatre of operations and the events leading up to the conflict situation. They specify the international setting and the attitudes of allies, allies of the enemy and neutrals. They also detail the political aims of the Australian government and its military strategic objectives. All strategic scenarios, taken together, in principle largely define overall defense requirements.

Australia's strategically derived operational scenarios are reference scenarios that have been extended from strategic scenarios, to provide sufficient detail for rigorous evaluation and descriptions of defense requirements for and use of capabilities. One scenario example is evicting an enemy from an overseas territory with phases representing the buildup, the establishment of sea and air dominance, lodgement, the tactical battle, and the post-battle phase. The Australian operational scenarios are more

detailed extensions of the strategic scenarios, often detailing a force structure with equipped capabilities to be applied to achieve the particular mission. Strategic and operational scenarios form a link between strategic planning, futures analysis, experimentation, capability development, force development, contingency planning and preparedness.

The United Kingdom Ministry of Defence builds in what it calls "concurrency" in its use of scenarios for force structure development. The Ministry of Defense establishes what is needed for a particular operational scenario and then maps the conclusions against a number of operations that should be conducted at any one time. For example, the United Kingdom should be able to respond to a medium scale operation at the same time as an enduring small scale operation and a one time small scale intervention operation.

The Canada Department of National Defence uses operational research tools in a scenario operational capability risk assessment model to identify how often different types of capabilities are called upon in the scenarios. While there are arguments for using a broad range of scenarios in CBP to thoroughly test force structure for a wide range of situations, the Department of National Defence argues for a small number. The Department believes that while a more comprehensive list of scenarios may theoretically add more precision to the force planning process, they may not as there are so many uncertainties.

Thus, the defense community emphasizes that defense capability should be assessed by using plausible situations in planning scenarios to cover the full spectrum of military activities. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur. Many state and local officials are concerned that the national planning scenarios focus too much on terrorism and, as mentioned above, the scenarios do not include different timeframes, including very long term.

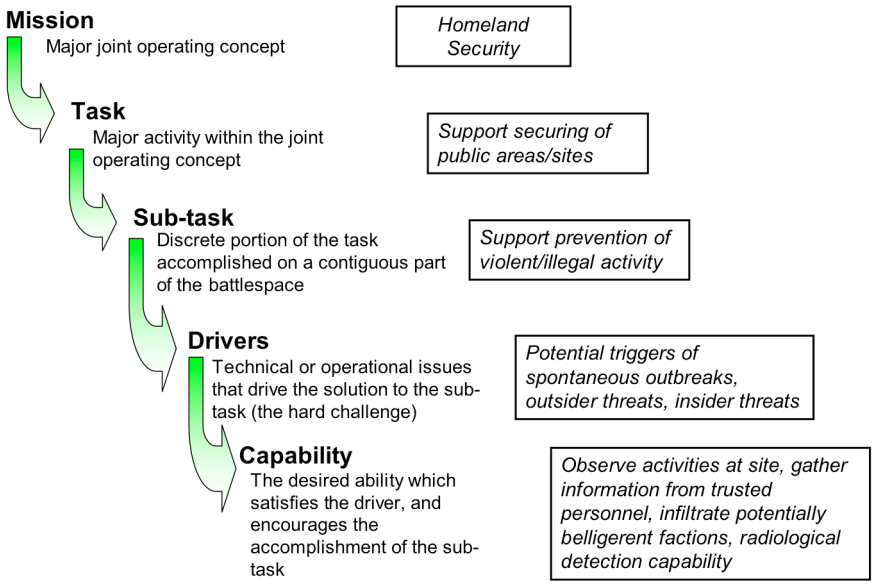
The homeland security CBP approach makes the assumption that preparing for terrorist events, representing the vast majority of the planning scenarios, will prepare jurisdictions for all-hazards events. Many would argue that it might make more sense to develop capabilities for more probable all-hazards that can be "ramped up" for large-scale terrorist events or large-scale natural or non-intentional human-caused disasters. As a result, capabilities would cover a full spectrum of homeland security activities. Capabilities then could be scaled to what is affordable and sustainable (and more likely to be used) at the state and local level, and then supplemented by regional and/or federal capabilities if an event overwhelms those capabilities. This approach anticipates that in most catastrophic situations, even a full complement of capabilities at the local or regional level will be quickly overcome.

Capability Development and Standard Categories

A ninth component is providing guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate. For example, the DoD's Battlespace Awareness Functional Capabilities Board provides guidelines to craft capability descriptions. The descriptions must indicate 1) what the capability is to do, such as "track" or "determine," 2) identify a target or subject, such as a person on a battlefield, 3) the size or range of the subject, such as a large vessel, 4) the

domain of the target systems, such as air-breathing targets, 5) the area of action, and 6) the range to area, or the distance over which effects must be made or action taken. Capabilities are seen as the end of a "waterfall" of lower levels of mission used in functional area analysis, illustrated in Figure 2.

Figure 2. Battlespace Awareness Waterfall Example



Regarding categories, the TCP recommends standard groupings such as capability clusters or capability partitions to make the CBP process more manageable. There are many ways to define the boundaries between capability partitions. These partitions are based on the ability to perform tasks, or to deliver effects, such as the control and denial of underwater battle space. A key enabler for successful CBP is getting the partitions agreed to by the key stakeholders and account for synergies and dependencies across partitions. The capability partitions should not be aligned to inappropriate organizations. If they are aligned, then organizational stovepiping is encouraged.[5]

It is suggested at least two fundamental military capability categorization options can be used independently or in combination. One is functional or means-focused. These capabilities would include battlespace awareness, command and control, logistics, and force management. Another option is operational or ends-focused. Operational categories might include strategic deterrence, homeland defense, civil support, and land combat operations. Each category then would be further defined. To illustrate, force management would include force employment and force deployment. Homeland defense would include capabilities such as continuity of operations, securing domestic approaches and territory, and population protection.[6]

The defense communities have taken similar approaches to capability categorization. For example, as described by the United Kingdom Ministry of Defence, military tasks

provide a framework for detailed defense planning for the size, shape, and capabilities of the United Kingdom's Armed Forces. The military tasks reflect the broad types of tasks and operations in which the United Kingdom is likely to be involved and then provide an output-focused framework for developing force structure requirements. The eighteen military tasks are in the four areas of 1) standing strategic commitments, such as nuclear deterrent and strategic intelligence gathering, 2) standing home commitments, such as security at home in support of other government departments, 3) standing overseas commitments, such as commitments to international alliances and partners, and 4) contingent operations overseas, such as humanitarian assistance and peace support operations. Military capability is divided into six key capability elements, such as maritime, land, and logistics. The Canada Department of National Defence divides military tasks into eight capability areas, such as Command, Information and Intelligence, and Corporate Policy and Strategy.

The defense community experiences indicate that an important component is providing guidance on crafting capability descriptions and developing standard capability categories fully reflecting what effects the capabilities should generate. DHS policies and guidance do generically define a capability, but guidance is lacking as to how to craft a capability description. The homeland security capability categories should be agreed to by key stakeholders and account for interrelationships across the capability categories.

At present, there does not appear to be a clear sense and rationale as to the best way to partition the homeland security capabilities for use by most entities. The task list categories, still in draft, initially indicated capabilities will reflect primarily an indirect organizational categorization—federal, state, and local responsibilities, and then later on those for the private sector, nongovernmental organizations, and citizens. This may have created organizational stovepiping of capabilities, which the defense community cautioned against. The latest draft documents use "mission areas" for emphasis—prevention, protection, response, and recover. The IED prototype uses mission areas with critical tasks drawn from the organizational tasks lists, adding to the confusion of what categories are in play or may be the final form. The categorization across task lists and capability areas should be clarified, justified, and stabilized.

Decision Rules for Lists

In another component, the defense communities establish clear rules for the development of task lists and capability lists. These rules include the source for compiling the lists, what criteria will be used in selecting candidates for the list, and how they should be arrayed. For example, the universal joint task list for DoD's CBP is the result of fourteen years of spiral development. Many sources of information from the task list to individual service sources to interagency information regarding tasks, conditions, and standards are being filtered for DoD's universal capability library. The library structure consists of a capability library—a master database of capabilities linked to current, planned, and roadmapped forces, units, and equipment—and a task library. The task library is the master database of all doctrinal and conceptual tasks.

The Australia Department of Defence has followed several principles for designing its Australian Joint Essential Tasks: joint, enduring, essential, and containing relevant and current content. Joint tasks are those that require the contribution of two or more forces working together to achieve the desired outcome. Enduring tasks capture how the

Australian Defence Force operates currently and might undertake joint operations in the future. Essential tasks capture what are required for the conduct of an operation.

In addition to the design principles, Australia Department of Defence has set two further design goals for future Joint Task development—uniqueness and hierarchical. For any given level of command, a task only appears once in the task hierarchy. No tasks should be duplicated, although some related tasks might appear in more than one place. The requirement for uniqueness is analogous to the United States' UJTL requirement that tasks be mutually exclusive, that is, that any task performed by any joint organization or service unit will fit into only one place in the task structure. Thus common tasks were abstracted out of their natural parent task and were grouped together.

In addition, the Joint Tasks, similar to other defense agencies, are intended to maintain a hierarchical structure. For a high level task, its subordinate tasks, taken together, comprehensively define all of the activities in the higher-level task. For example, the Australian Joint Tasks and Canada's joint task list have three levels of joint tasks—strategic, operational, and tactical. The tasks within each level are further disaggregated into two additional layers of sub-tasks with each layer more detailed and specific.

However, opinions differ about hierarchical and uniqueness design for the lists. Some recommend that hierarchies should not be imposed because these require preconceived notions about what criteria are more valuable or useful for segregating data. Hierarchies require frequent changes or alternate versions of lists. Mutual exclusivity also may not be required, at least at the operational level as no real force, unit, equipment, or system falls entirely within any one category.

To summarize, the defense communities establish clear rules for the development of task lists and capability lists, such as uniqueness and hierarchy. For homeland security, publicly available documents indicate a lack of explicit rules for decision-making. As part of CBP implementation, DHS could easily formulate such rules. Explicit decision rules should help the further development and revision of the detailed and lengthy lists over time. For example, a rule regarding uniqueness would ensure developers would independently assess each task and whether its description is similar to or actually part of another task.

CBP Evolution

Another component is evolving CBP depending on planning applications and maturity. Each defense organization is in various stages of implementing CBP, both on a national joint and individual service level. However, each organization has tailored CBP and taken a staged approach to implementation. For example, as described by the Australia Department of Defence, allied CBP approaches are similar, but emphasize different outcomes over time:

- The United Kingdom has primarily focused on immediate operations and long term planning. The United Kingdom has used a list of essential joint tasks as an analysis tool for exercises with more recent efforts to integrate the tasks into mission analysis and operational planning.
- Canada's tasks are closely linked into force planning scenarios and future planning and are used in joint department structuring so each department uses the same criteria for operations and to translate tasks into capability. Canada uses its joint task list

for force employment and capability development and has developed eleven force planning scenarios to link their capability development and planning.

- The United States joint task list has aided in the development of planning requirements for joint exercises since 1993. The joint task list was developed specifically for training but is now linked into readiness and preparedness reporting and capability development.

CBP also will progress at a different pace in the organization, creating different levels of maturity overall. Thus, some capabilities needed for the defense community of a nation may be delayed compared to others. The Canada Department of National Defence points out that over time CBP improves commonality among defense planners by introducing a common way of describing and discussing capability elements. As the different national defense organizations in Canada adopt the common terminology, it becomes easier to link different plans providing various capability components. In the beginning, certain plans will be more mature or more vital for integrated planning. Canada's long-term plan for major equipment is the most mature in employing CBP. The development of long-term plans for personnel resources, research, concepts, information technology, and infrastructure is likely necessary before more encompassing capability planning can be done in Canada.

Thus, the defense community experience includes evolving CBP to reflect planning applications. CBP will progress at a different pace in different parts of the organization, creating different levels of maturity. For homeland security, current policy timeframes have precluded a more evolutionary approach to CBP and imposed extremely limited turnaround time for stakeholder comments on various draft products. DHS does plan on enhancing the approach, but it will be very hard to dismantle earlier structures once the homeland security grant process "institutionalizes" around capability categories and tiered requirements. A comprehensive CBP system is expected to be up and running in a timeframe of months. While adoption initially will be based on one scenario—explosive devices—for initial planning, federal funding guidance indicates that in less than two years, all scenarios will be part of state and local planning. In addition, the CBP as currently being adopted does not directly address differing maturity in capability areas that may impede overall progress in homeland security preparedness. DHS would be well-served to consider such maturity considerations in its CBP implementation decisions.

CBP Enablers

The last component is additional organizational and cultural enablers for effective CBP adoption. These are other necessary and sufficient factors, which along with components already mentioned, such as stakeholder ownership, create and sustain the environment for implementation. Many practitioners and students of CBP have highlighted considerations for CBP design and deployment that cover a wide range of factors, from mindset changes to the practicalities of resourcing CBP planning and execution.

Davis and Jenkins write that CBP's complexity requires a passion for adaptiveness and substantial analysis leading to a combination of incentives, standards, and policies for CBP.[7] They cite the need for major studies on how to modify economic and other incentives to encourage more adaptive and recoverable systems. Feaga recommends developing new languages in risk management and effects once it is known what

capability proficiency and sufficiency levels are needed.[8] The Australian experience indicates attention is needed to address conflicting processes, the lack of suitable analytical tools, excessively prescriptive requirements, and the recognition of functional linkages and dependencies between related capabilities.

Similarly, DoD recommends a broad and long-term strategic perspective, a greater appreciation of the operational and strategic environmental factors, and a rigorous analysis of the capabilities needed to achieve defense policy goals. The Technical Cooperation Program lists the need for consistent cost estimates and resource provision for both the development and execution of the CBP process. Moreover, joint force personnel will require a joint and expeditionary "mindset" reflecting a greater level of deployability and versatility to avoid organizational stovepiping. Canada's Department of National Defence identifies the challenge of developing and maintaining capabilities to conduct operations independently in domestic situations and alongside alliance and coalition partners for international obligations. Canada believes the focus must remain on combat-capable units because these units can be employed in other security activities, such as peacekeeping, while those with non-combat capabilities cannot meet combat needs.

Therefore, additional organizational and cultural enablers are needed for effective CBP adoption. The defense experience indicates many facilitative factors come into play for effective CBP, many analytical and skill-based, but others such as incentives, the rationality of processes, and a deliberative approach. For homeland security, enablers such as these may be recognized but have not been adequately addressed, perhaps because they are the difficult "softer" issues or the assumption is that they will be dealt with by stakeholders individually. In addition, the rapid spiral development process has forestalled more careful consideration of CBP and what is needed to support its successful implementation.

CHALLENGES IN ADOPTING THE DOD APPROACH

While this article has highlighted many components important to CBP implementation if the DoD experience is the model, DHS will face further challenges in implementing CBP. My analysis indicates that four key factors differentiate homeland security and the national defense mission that will pose challenges for DHS adoption.

Mission Scope and Coverage

A first challenge is mission related. In defense, the **mission scope** is more clearly defined for national defense, most often military action and civil support. While many rightly argue that the national defense mission has broadened considerably in recent years, for homeland security, the mission is arguably broader for prevention, vulnerability reduction, and response and recovery responsibilities. Actions are required at home and abroad, from dealings with individual citizens to negotiations with nation-states as border protection is extended overseas. Homeland security also stresses all-hazards preparedness, requiring attention to a wide range of events, from small-scale earthquakes to catastrophic terrorist events. CBP should allow Homeland Security to consider these multiple and diverse missions, the common and unique capabilities they require, and what tradeoffs in priorities and resourcing might be necessary.

In addition, the defense experiences emphasize **full mission coverage**. At present, it is not clear if the homeland security CBP approach is emphasizing prevention and deterrence. While draft DHS task lists have included prevention efforts such as intelligence development and providing strategic and threat intelligence, the task lists focus much more attention on vulnerability reduction and response and recovery. Emergency response—after an event—appears to take the lion's share of analysis and preparation with clear emphasis on first responder roles and responsibilities.

The constrained homeland security mission scope and coverage may be the result of several factors. Gilman observed that there has been a major DHS focus on weapons of mass destruction and terrorism, and not on all hazards and events that happen all that time, such as explosions.[9] Prevention has been "under the radar screen" for DHS as it might be considered the purview of other agencies, such as the Department of Justice or the Central Intelligence Agency, or state and local law enforcement officials. In addition, DHS' Office for Domestic Preparedness has had a mission of emergency management, not other aspects of homeland security, and it would be normal to see this office maximize its area of strength or understanding. Perhaps more importantly, since September 11, first responders have been front and center, their needs expounded, and the results in terms of new equipment and capabilities much more visible.

Organizational Perspectives

A second challenge involves organizational perspectives. One perspective is a **federal department versus a national view.** The defense community normally contains decisions within a cabinet department and White House sphere, with input from other federal agencies and to a lesser extent, international partners. In contrast, homeland security is presented as national in scope, not a federal responsibility of primarily just one executive department or agency. A national perspective requires a much more collaborative approach, particularly in a federalist system, and a fairly clear distinction between public and private spheres.

Moreover, even within the federal homeland security establishment there is fragmentation. Federal agencies other than DHS can act autonomously, buoyed by their own sources of support and direction. Even when collaborative decisions are made, the vehicles for enforcement are very limited or unwanted. The homeland security organizations represent different disciplines and perspectives, levels of public, private, and nongovernmental organizations, and even horizontal relationships such as the involvement of different federal, state, or local cabinet agencies. Defense has a central core of military services that perform its activities that share a common culture and perspective to support and deploy the warfighter. CBP should allow Homeland Security to change its unit of analysis from organizations and requirements to capabilities and their delivery.

In addition, **chain of command and exercise of authority** are different. Defense normally has a top-down command and control structure with a highly disciplined attention to authority. The homeland security CBP approach at present does not adequately guide analysis when assets and capabilities to accomplish a mission are not under one jurisdiction, may be unknown, or may ebb and flow over time. The draft national preparedness rating scheme indicates that a group of organizations can be rated

collaboratively under a mutual aide or an assistance compact to perform prevention, response, or recovery tasks for a specific scenario.

For CBP, it is crucial that relationships are driven by strategic alliances among equal partners where all stakeholders—strategic partners—are identified, their needs clearly represented in collaborative decision-making, and incentives provided for decisions not to unravel. Capability planning is always tied to sustainability analyses and funding support favors multiple-use capabilities and multiple sources of capabilities to reduce the funding burden on any one organization. Additional work is needed to better understand how to apply the framework where there are networks of organizations that work homeland security issues or are discrete sets of organizations that handle specific homeland security functions. Contingency planning is necessary in the event individual organizations or sectors will not meet their capability obligations. This will be even more important when the CBP framework is expanded to address private sector and nongovernmental organizations who are critical players in prevention, vulnerability reduction, and response and recovery strategies and actions.

Resource Development and Leveraging

A third challenge is the resources that can be brought to bear for homeland security in contrast to the defense community. To start, resource leveraging requires the **understanding of assets** that compose capabilities and in general what they can accomplish. Capabilities include a diverse selection of elements, such as plans, procedures, personnel, equipment, and activities. Defense organizations have paid considerable attention to the assets that can be combined for capabilities, where they are deployed, what their maintenance or skill condition is, and when they will become obsolete or require renewal. This is not yet the case in homeland security, where asset identification and control is dispersed to thousands of organizations who may or may not have a complete and accurate inventory. Many homeland security contingency plans draw on mutual aid or regional agreements, often without full identification of assets and how they will work together. CBP provides a mechanism for asset identification, but initially CBP will be hampered as Homeland Security officials gather and assess this information and their contribution to capability planning.

In addition, resources include **planning resources, skills, tools, and experiences**. Defense communities normally have decades, if not centuries, of planning experience for concrete events and contingencies. These communities bring to bear a wide range of tools such as wargaming, exercises, and simulations, and a small army of skilled and experienced planners devoted to such work. Exercises and actual field experience are rapidly fed back to planners. In contrast, homeland security is in the early stages of planning and is often not well-resourced with dedicated staff, particularly in smaller jurisdictions. Tools and skills are still in development in government organizations. While emergency exercises have been the norm for a number of years, a systematic collection, evaluation, and dissemination of lessons learned and better practices has only recently picked up speed. The private sector in some critical infrastructure areas and for some companies, may have the requisite resources, skills, tools, and experiences, or can draw on combined sector practices, but not all. Non-governmental organizations, with limited resources, may also have difficulty in adopting CBP. It can be expected there

will be a slower identification of current and required capabilities and under what scenarios they are effective.

A tiered CBP approach in homeland security may not adequately address the very wide variety of structures, skills, and processes for homeland security activities across the nation. For example, Gilman noted that DHS does not understand, or chooses not to understand, that there is a major difference in homeland security or emergency preparedness operations and capacities between the rural and urban areas in a state or region.[10] He said that many homeland security and emergency management contacts are in rural areas, and many are volunteers or handle homeland security along with many other tasks. These officials often have limited infrastructure support, such as access to good communication services. Rural areas also have more difficulty forming mutual aid compacts and, if they do, may get limited help because of geography or limited regional assets and liabilities. Rural areas may have to wait many hours for mutual aid help to arrive because of the distances involved.

Target Audience

A final challenge is the differences in the target audiences for CBP. For the defense community, the clear customer for CBP outputs is the combatant commander who must carry out the defense missions and relies on mission capability packages. For homeland security, the target audience at present is broadly described by DHS as the "homeland security community," which can cover federal, state, local, private, and nongovernmental organizations, and even to the level of the individual citizen. Thus, there is not a discrete set of homeland security "combatant commanders" under the current DHS CBP approach. This has added to the complexity and confusion surrounding CBP that will require further attention.

Federal national policy is primarily directed at state and local jurisdictions at this time, with some attention paid to limited regional compacts. It may be that CBP development over time will clarify that the combatant commander should be those state and local government officials responsible for direct prevention, vulnerability reduction, and response and recovery activities. While private sector and non-governmental officials have direct homeland security responsibilities as well, the CBP process may need to stop at the governmental level. Governmental CBP outputs can be planning inputs to these other jurisdictions for their own planning processes.

Instead of supporting the combatant commander, the capabilities-based approach might get bogged-down in a checklist mentality of responding to lists of many tasks represented by the UTL (Universal Task List) and a targeted list for critical capabilities. "Checking off" the tasks forces attention to discrete activities, and not to capabilities and homeland security results for an organization and its homeland security partners. State and local officials at the October 2004 capabilities workshop noted that the task lists and defined capabilities can easily become a standard of care to which they will become individually accountable. A defensive posture might be to manage to the lists, and not to the overall results that must be achieved within a risk assessment decision-making process. As a result, developing envelopes of capability for specific operational challenges for the combatant commander will be lost.

[1] The White House, *Homeland security presidential directive/HSPD-8* (Washington, DC: The White House, December 17, 2003).

[2] C. Kelley, P. Davis, B. Bennett, E. Harris, R. Hundley, E. Larson, R. Mesic, and M. Miller, *Metrics for the quadrennial defense review's operational goals* (Santa Monica, CA: RAND National Defense Research Institute, 2003); P. Davis, *Analytical architecture for capabilities-based planning, mission-system analysis, and transformation* (Santa Monica, CA: RAND, 2002).

[3] The Technical Cooperation Program, *TTCP technical report: Guide to capability-based planning* (2004) http://www.mors.org/meetings/cbp/cbp_presentations.htm (accessed October 19, 2004).

[4] The defense community sources drew on material from the Australia Department of Defence, the Canada Department of National Defence, the United Kingdom Ministry of Defence, the United States Department of Defense, The Technical Cooperation Program, and individual papers and presentations.

[5] B. Taylor, *Guide to capabilities-based planning*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

[6] T. Kiefer, *Capabilities based planning framework*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

[7] P. Davis and B. Jenkins, *Deterrence and influence in counterterrorism: a component in the war on al Qaeda* (Santa Monica, CA: RAND National Defense Research Institute, 2002).

[8] K. Feaga, "The USAF capabilities based CONOPS construct," Academic research paper, U.S. Army War College (2004).

[9] J. Gilman, "Using a performance management system for homeland security funds to demonstrate accountability and improve organizational effectiveness," Presentation to the Advanced Learning Institute's Performance Measurement for Homeland Security conference, Arlington, VA (December 1, 2004).

[10] Ibid.